InvestiGO
Revista Científica Multidisciplinaria
ISSN 2953-6367
http://revistainvestigo.com

julio - diciembre 2025
Vol. 6, No. 16, PP. 602-616
https://doi.org/10.56519/s4q06357

LOS BENEFICIOS DE UNA AUDITORIA INFORMÁTICA

THE BENEFITS OF AN IT AUDIT

Luis Andrés Hidalgo Bonifaz[1], Esteban Xavier Chiliquinga Cevallos[2]

{andres.hidalgo@upec.edu.ec[1], esteban.chiliquinga@upec.edu.ec[2]}

Fecha de recepción: 07/06/2025 / Fecha de aceptación: 16/06/2025 / Fecha de publicación: 01/07/2025

RESUMEN: La creciente dependencia de las organizaciones hacia los sistemas de información plantea desafíos en materia de seguridad, eficiencia y cumplimiento normativo que amenazan la sostenibilidad y competitividad institucional. En respuesta a estos retos, la auditoría informática se posiciona como una herramienta estratégica fundamental para identificar, gestionar y mitigar riesgos asociados a la operación tecnológica en entornos cada vez más digitalizados. Esta investigación analizó en profundidad los beneficios derivados de la aplicación sistemática de auditorías informáticas, mediante una revisión documental y comparativa de literatura científica, informes técnicos, estándares internacionales y casos de estudio recientes en Latinoamérica. Se empleó una metodología cualitativa de análisis temático, complementada con datos cuantitativos sobre la evolución de incidentes de seguridad, ahorro operativo y éxito regulatorio después de la adopción de prácticas de auditoría. Los principales resultados demostraron una reducción significativa en la ocurrencia de incidentes críticos, mejoras en la eficiencia operativa y una mayor capacidad de cumplimiento normativo y obtención de certificaciones, beneficiando tanto a empresas como a instituciones públicas. Igualmente, se identificaron desafíos, tales como la necesidad de capacitación constante para los auditores, adaptación metodológica a contextos locales y superación de resistencias internas. Las conclusiones refuerzan el argumento de que la auditoría informática, lejos de ser un gasto operativo, es una inversión esencial que impulsa la innovación, la seguridad y la confianza organizacional, recomendando su adopción bajo marcos normativos actualizados y una cultura de mejora continua.

Palabras clave: Auditoría informática, cumplimiento normativo, eficiencia organizacional, ciberseguridad

ABSTRACT: The growing dependence of organizations on information systems presents challenges in security, efficiency, and regulatory compliance that threaten institutional sustainability and competitiveness. In response, information systems auditing stands out as a

[1]Profesor ocasional de la Carrera de Computación, Universidad Politécnica Estatal del Carchi, Ecuador, ORCID https://orcid.org/0000-0003-3635-5877; +59388129942.
[2]Profesor ocasional con gestión en Posgrado, Universidad Politécnica Estatal del Carchi, Ecuador, https://orcid.org/0009-0003-1909-8597; +593986236676

fundamental strategic tool for identifying, managing, and mitigating risks associated with technological operations in increasingly digitalized environments. This article deeply analyzes the benefits of systematically implementing IS audits through a thorough literature review, technical reports, international standards, and recent case studies from Latin America. A qualitative thematic analysis methodology was employed, supplemented with quantitative data on the evolution of security incidents, operational savings, and regulatory success after audit adoption. The main results demonstrate a significant reduction in critical incidents, improvements in operational efficiency, and a greater capacity for regulatory compliance and certification, benefiting both private companies and public institutions. The study also identifies challenges such as the need for continuous auditor training, methodological adaptation to local contexts, and overcoming internal resistance. Conclusions highlight that IS auditing, far from being an operational expense, constitutes an essential investment driving innovation, security, and organizational trust, and recommend its adoption under updated normative frameworks and a culture of continuous improvement.

Keywords: Information systems audit, regulatory compliance, organizational efficiency, cybersecurity

INTRODUCCIÓN

La rápida expansión de las tecnologías de la información y la comunicación (TIC) ha transformado de forma radical las operaciones, servicios y la toma de decisiones tanto en organizaciones privadas como públicas en Latinoamérica y el mundo (1), (2). Actualmente, la dependencia de las empresas e instituciones respecto de sus sistemas informáticos es total, pues constituyen la columna vertebral para procesos críticos, flujos de información, automatización de tareas y la gestión eficiente de recursos (3). Esta centralidad tecnológica ha impulsado la productividad y nuevas formas de interacción, pero también introduce nuevas vulnerabilidades. El grado de digitalización alcanzado trae consigo amenazas tecnológicas cada vez más sofisticadas, globales y persistentes, las cuales afectan directamente la seguridad, la continuidad del negocio y la reputación institucional (4), (5). Incidentes como fugas de información, ciberataques, ransomware o fraudes internos demuestran el potencial de impacto de los riesgos tecnológicos en la salud organizacional, evidenciando la necesidad de controles, vigilancia y mejora continua de los procesos informáticos.

En este contexto, la auditoría informática surge como una disciplina especializada, fundamental y estratégica para identificar y gestionar riesgos asociados a los sistemas de información actuales. La auditoría informática tiene un enfoque integral que trasciende la simple revisión de controles técnicos, abordando la validación de la integridad, disponibilidad y confidencialidad de los activos digitales, así como el fortalecimiento de la toma de decisiones basada en evidencia objetiva. Su alcance no se limita únicamente a evaluar la seguridad de los sistemas, sino que también incorpora el análisis de la eficiencia y la confiabilidad de los procesos tecnológicos internos, la optimización de recursos, el aseguramiento del cumplimiento normativo y la alineación estratégica de las tecnologías con los objetivos organizacionales (3), (6). A diferencia

de la auditoría tradicional, la auditoría informática exige conocimientos técnicos avanzados sobre infraestructura de redes, desarrollo de software, bases de datos, ciberseguridad, legislación TIC y el dominio de marcos regulatorios internacionales como ISO/IEC 27001, COBIT, NIST, MAGERIT o el Reglamento General de Protección de Datos (GDPR), entre otros (2), (7).

El valor de la auditoría informática adecuada radica no sólo en la prevención efectiva de ataques y fraudes internos o externos, sino también en su capacidad para ofrecer recomendaciones específicas y accionables que permitan mejorar la eficiencia operativa, detectar debilidades antes de que deriven en incidentes y fomentar una cultura organizacional orientada a la gestión proactiva del riesgo (1), (8). Múltiples investigaciones han evidenciado que la implementación sistemática de auditorías informáticas genera descensos significativos en la ocurrencia de incidentes críticos, reducciones en los costos asociados a la recuperación post-incidente y un aumento sustancial en la conformidad regulatoria, traduciéndose todo ello en ventajas competitivas y confianza ante clientes, socios y reguladores (4), (6).

No obstante, la auditoría informática enfrenta desafíos sustanciales derivados del crecimiento exponencial de la digitalización, el uso imparable de la computación en la nube, la virtualización de infraestructuras, la proliferación del Internet de las Cosas [IoT] y la emergencia de riesgos éticos y legales asociados al uso intensivo de inteligencia artificial y analítica de datos. Estos retos se ven agravados por la escasez de profesionales altamente calificados y la necesidad permanente de mantener un nivel de actualización elevado para anticipar y responder eficazmente a nuevas amenazas (7). Todo ello subraya la importancia crítica de instaurar auditorías informáticas sistemáticas, adaptativas y en consonancia con los cambios del entorno digital.

El objetivo de esta investigación es analizar exhaustivamente los beneficios tangibles e intangibles de la auditoría informática en la gestión de la seguridad, la eficiencia operativa y la conformidad normativa dentro de organizaciones modernas de diversos sectores. Para ello, se utilizó una revisión sistemática de literatura científica reciente, informes técnicos especializados, casos de estudio y la comparación de resultados obtenidos en instituciones que han implementado auditorías periódicas en sus sistemas de información (8). El trabajo aborda las mejores prácticas internacionales, los retos actuales y las tendencias futuras, y pone en evidencia la importancia de considerar la auditoría informática como un elemento esencial no sólo para la sostenibilidad, sino también para la innovación y la competitividad a largo plazo. La estructura de este artículo contempla una revisión profunda del marco normativo y metodológico, el análisis de resultados cuantificables en empresas y organismos públicos, la discusión sobre los hallazgos principales y una propuesta de recomendaciones prácticas para la adopción efectiva de auditorías sistemáticas y proactivas en el entorno digital contemporáneo.

MATERIALES Y MÉTODOS

Para garantizar la calidad de la revisión sistemática de la información recolectada y la transparencia metodológica, se adoptaron principios establecidos en protocolos internacionales

para revisiones sistemáticas, especialmente las guías PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses), adaptándolos al alcance temático del presente trabajo (1), así como las pautas recomendadas para revisiones de literatura científica en ciencias sociales y administración (2).

Durante la primera fase, la estrategia de búsqueda incluyó la consulta exhaustiva en bases de datos científicas internacionales ampliamente reconocidas por su rigor y alcance multidisciplinario, como Scopus, Web of Science, Redalyc y SciELO, además de repositorios especializados como Dialnet y Google Scholar. Para cubrir literatura regional relevante y evitar sesgos de ubicación, se priorizó la inclusión de artículos indexados en proyectos de investigación latinoamericanos publicados entre 2015 y 2024 (3). Adicionalmente, se examinaron tesis de maestría y doctorado, libros, manuales técnicos y documentos regulatorios emitidos por organismos internacionales de referencia en el ámbito de la auditoría informática y la gestión de riesgos tecnológicos, tales como ISACA, INCIBE, INTECO e ISO (4), (5).

La definición precisa de términos de búsqueda fue fundamental para asegurar la pertinencia y exhaustividad de la revisión. Se utilizaron palabras clave como: “Auditoría informática”, “beneficios”, “gestión de riesgos”, “cumplimiento normativo”, “ISO 27001”, “COBIT”, “ciberseguridad”, además de operadores booleanos ("AND", "OR", "NOT") y estrategias de búsqueda cruzada para ampliar los resultados y cubrir distintas combinaciones temáticas según las recomendaciones de Delgado-López y Luna (2). De manera complementaria, se realizó un rastreo manual de referencias citadas en los artículos sintetizados, con el fin de identificar literatura relevante no indexada directamente en los buscadores empleados.

Los criterios de inclusión se basaron en la pertinencia temática, es decir, trabajos que abordaran de forma sustantiva auditoría informática o auditoría de sistemas de información, con énfasis en gestión de riesgos, mejoras de eficiencia y cumplimiento normativo. Se priorizaron publicaciones recientes (últimos 5 años) y aquellas que presentasen diseño metodológico transparente, evidencia empírica, estudios de casos, o análisis comparativos útiles para entornos empresariales, públicos o mixtos (6). La exclusión se aplicó para investigaciones enfocadas exclusivamente en auditorías financieras clásicas, trabajos conceptuales sin validación práctica y artículos repetidos en diferentes bases. Igualmente, se descartaron publicaciones sin revisión por pares o cuyos resultados carecieran de aplicabilidad en los contextos de interés analizados (América Latina, Europa y Estados Unidos).

En la segunda etapa, la información recolectada fue extraída por medio de matrices comparativas temáticas que permitieron sistematizar los contenidos y facilitar su análisis. Para cada fuente seleccionada, se identificaron elementos clave como definiciones operativas de auditoría informática, principales marcos normativos reportados (ISO/IEC 27001, COBIT 5, NIST, MAGERIT, GDPR), metodologías de ejecución, resultados cuantitativos y cualitativos derivados de auditorías implementadas, así como retos y oportunidades observados en los sectores evaluados (5), (7). Además, se consideraron informes sectoriales sobre incidentes de seguridad informática, la frecuencia y gravedad de riesgos mitigados y el impacto en la optimización de recursos luego de la puesta en marcha de auditorías regulares (8).

En la fase de análisis, se empleó un enfoque cualitativo, utilizando técnicas de análisis temático para la identificación, organización y categorización de los beneficios de la auditoría informática, tanto tangibles (por ejemplo, disminución del número de incidentes, reducción de costos, obtención de certificaciones) como intangibles (mejora en la confianza institucional, reputación, cultura de cumplimiento y de seguridad) (1), (9). Cuando la literatura y los informes de caso lo permitieron, se complementó el análisis con datos cuantitativos descriptivos para comparar la frecuencia y gravedad de fallas tecnológicas, los impactos económicos y el grado de satisfacción de usuarios internos y externos tras la implementación de auditorías.

Para robustecer el rigor metodológico y minimizar sesgos, se aplicó triangulación de fuentes, contrastando hallazgos entre artículos académicos, reportes técnicos, guías metodológicas oficiales y experiencias directas documentadas en informes de auditoría de organismos internacionales y latinoamericanos (4), (6), (10). De igual forma, se supervisó la calidad de los estudios incluidos mediante la revisión de la claridad en la exposición metodológica, la justificación de muestras y la presentación de limitaciones, siguiendo parámetros sugeridos por expertos como Moher *et al*. (19 y Lozano *et al.* (9).

Como complemento, se elaboraron tablas y gráficos propios a partir de la información sistematizada en la revisión, lo cual permitió comparar, resumir y visualizar los principales beneficios identificados en el corpus documental. Estos instrumentos actúan como soportes visuales y analíticos para facilitar la interpretación de los resultados expuestos en las secciones siguientes.

Finalmente, los límites y alcances de la presente revisión han sido explicitados conforme a los lineamientos internacionales y las buenas prácticas recomendadas en la literatura científica, garantizando transparencia, replicabilidad y utilidad para futuras investigaciones sobre auditoría informática aplicada a la gestión organizacional (1), (9).

RESULTADOS

Los resultados obtenidos a partir de la revisión exhaustiva de literatura científica, informes técnicos y experiencias empíricas permiten identificar una serie de beneficios tangibles e intangibles, así como desafíos específicos en la aplicación de auditorías informáticas en organizaciones contemporáneas. A través del análisis profundo de estudios académicos recientes, casos sectoriales y reportes técnicos, estos resultados evidencian el impacto multifacético de la auditoría informática en la seguridad, la eficiencia, el cumplimiento normativo y la resiliencia de las estructuras organizacionales.

Reducción de riesgos e incidentes de seguridad informática

Uno de los hallazgos más reiterados es la capacidad de la auditoría informática para reducir de forma sustancial los riesgos y prevenir incidentes de seguridad. La literatura revisada confirmó

que organizaciones pertenecientes a sectores críticos como el financiero, salud, educación, manufactura y gobierno logran disminuir patrones de amenazas, vulnerabilidades explotadas, y exposición frente a ciberriesgos una vez implementan auditorías regulares bajo metodologías como ISO 27001, COBIT 5, NIST o MAGERIT (1), (2), (3), (7), (8).

Jimbo-Santana *et al*. reportan que, en el sector bancario y financiero latinoamericano, la frecuencia de incidentes críticos tales como accesos no autorizados, robo o pérdida de información estratégica y ataques de ransomware puede disminuir en un rango del 30% al 40% durante los dos primeros años de aplicación formal de auditorías, al comparar tasas históricas previas y posteriores a la instauración de programas de auditoría (2). Este descenso se atribuye a mejoras concretas en los controles de acceso lógico, segmentación de redes y robustecimiento de las políticas de backup, recomendaciones directas derivadas de auditorías con enfoque preventivo.

En instituciones de salud de la región andina, la revisión de la infraestructura y políticas por parte de equipos de auditoría interdisciplinarios ha permitido identificar brechas antes de ser explotadas, evitar fugas masivas de expedientes médicos, y optimizar la custodia y trazabilidad de la información clínico-administrativa (3), (4). Se destaca la importancia de la revisión periódica y su rol en evitar sanciones regulatorias: organizaciones auditadas cumplen más eficazmente con directrices de seguridad de la información sensibles, lo que refuerza la confianza de pacientes y entes reguladores.

Universidades ecuatorianas y peruanas, tras la implementación de auditorías sobre sus plataformas académicas, reportan contrastes notables en tentativas de intrusión, manipulación de calificaciones, y vulnerabilidad ante ataques de phishing masivo. Estos cambios han dado como resultados menores incidentes de pérdida de información estudiantil y una mejora sustancial en la estabilidad y reputación de los sistemas educativos digitales (5), (6).

En organismos de gobierno, la aplicación de modelos como MAGERIT ha fortalecido la gestión de riesgos y permitido corregir deficiencias críticas en políticas de acceso, control de identidades y administración de redes. Esto ha potenciado la transparencia institucional, reducido filtraciones de datos y mejorado la capacidad de respuesta frente a incidentes, que antes podían mantener vulnerables durante largos periodos los sistemas de nóminas, recursos humanos y finanzas públicas (6), (12).

La revisión sistematiza el aprendizaje colaborativo entre áreas de tecnología y auditoría, lo que ha permitido madurar la integración de controles y la gestión preventiva, evidenciando cómo el valor de la auditoría informática reside en su carácter anticipatorio y su capacidad para naturalizar en las organizaciones un enfoque de seguridad permanente (4), (9), (13).

Mejora en la eficiencia operativa y optimización de procesos

El segundo pilar identificado es la optimización de los procesos y la mejora de la eficiencia operativa como consecuencia de las auditorías informáticas. La literatura muestra que los

hallazgos, recomendaciones y acciones correctivas generadas a partir de auditorías sistemáticas propician la identificación de redundancias, automatización de operaciones, y consolidación de buenas prácticas que disminuyen errores humanos y costes operativos (7), (13).

Se evidencio que, en empresas de servicios y producción de México y Colombia, las acciones derivadas de auditoría informática han incentivado reorganizaciones estructurales capaces de producir ahorros de entre el 10% y el 22% en costos operativos de tecnología de la información en ciclos bianuales. Entre las acciones más comunes figuran la racionalización del uso de licencias de software, la planificación de compras y renovaciones, así como la optimización del almacenamiento digital.

En la banca latinoamericana estudiada por Jimbo-Santana *et al*., la estandarización de procesos, la documentación exhaustiva y la capacitación recurrente del personal minimizaron el impacto de los errores, disminuyeron el tiempo promedio de restauración de sistemas tras incidentes (de más de veinte horas a menos de catorce, por intervención de auditorías) y aceleraron la transferencia y asimilación de conocimientos entre personal de distintas generaciones (2).

El sector educativo se benefició del análisis automatizado de logs y minería de datos impulsados por recomendaciones de auditoría, permitiendo anticipar patrones de fallos y adaptarse proactivamente a los retos de plataformas virtuales en contextos de uso masivo y remoto (5), (6). Todo esto redundó en una reducción significativa de reclamaciones por fallas, mejor percepción del servicio por parte de usuarios internos y una mayor agilidad institucional frente a desafíos tecnológicos persistentes.

Asimismo, la revisión indica cómo la auditoría informática impulsa la adopción de marcos de trabajo ágiles en la gestión técnica, promueve la capacitación cruzada y la actualización continua y termina por reducir significativamente la dependencia del personal experto a través de la documentación y estandarización, elementos esenciales para la sostenibilidad operativa (8).

Fortalecimiento del cumplimiento normativo y logro de certificaciones

Otro beneficio crítico identificado es el cumplimiento normativo robustecido y la mayor capacidad para lograr y mantener certificaciones internacionales en gestión segura de la información. La complejidad de los marcos legales a nivel nacional y supranacional hace que la auditoría informática sea indispensable para las organizaciones que buscan demostrar conformidad con estándares como ISO/IEC 27001, PCI DSS, GDPR, Ley Orgánica de Protección de Datos (LOPD) y otras regulaciones de seguridad, privacidad y transparencia (10), (11).

INTECO reporta que la totalidad de empresas auditadas bajo requisitos de ISO/IEC 27001 alcanzó la certificación internacional sin hallazgos críticos, mientras que aquellas que optaron por auditorías puntuales fueron más propensas a recibir observaciones importantes por parte de los organismos certificadores externos (10). En el sector financiero y de salud, la evidencia de

cumplimiento generada por auditorías propició respuestas regulatorias más favorables, menores sanciones y el fortalecimiento de la relación con clientes, socios y entes fiscalizadores.

De manera transversal, la auditoría informática aporta claridad y trazabilidad sobre el ciclo de vida de los datos, desde su recolección, almacenamiento y procesamiento, hasta su destrucción segura. Documentar estos procesos y registrar el control de accesos y modificaciones permite responder rápida y eficazmente a requerimientos regulatorios y a solicitudes de titulares de la información, disminuyendo el riesgo de sanciones y demandas legales (4), (10).

La revisión también constata que las empresas certificadas presentan una mejor percepción social y reputacional, factor clave para la competitividad en mercados cada vez más exigentes en transparencia y ética digital (11).

Apoyo a la toma de decisiones estratégicas y gobierno corporativo

La dimensión estratégica de la auditoría informática reviste igualmente un papel fundamental en la gestión moderna. Más allá de su función técnica, la auditoría facilita reportes fundamentados y recomendaciones personalizadas que alimentan la toma de decisiones a nivel directivo y la planificación de inversiones (8). Plastino *et al.* señalan que la correlación entre resultados de auditoría y los indicadores de gestión de TI (tales como disponibilidad, resiliencia y eficiencia) permite priorizar acciones críticas, justificar presupuestos para innovación tecnológica y reducir resistencias a nuevos proyectos de transformación digital (8).

En los sectores bancario y asegurador, por ejemplo, la auditoría informática se convierte en la base argumental para la asignación de recursos en ciberseguridad, selección de proveedores homologados y adopción de políticas de trabajo remoto o híbrido, reforzando la gobernanza digital y la alineación estratégica entre alta dirección y equipos operativos (8), (11).

También se observó que la auditoría propicia el diálogo transversal entre departamentos y desarma silos organizativos, lo que facilita la comprensión de riesgos tecnológicos por parte de las áreas menos técnicas y fomenta un mayor involucramiento ejecutivo en las decisiones de innovación. La dinámica de mejora continua recomendada por los auditores fortalece así la madurez digital, la cultura de gestión del cambio y la proactividad institucional frente a nuevos riesgos emergentes (8), (13).

Generación de cultura organizacional de seguridad y gestión del cambio

Otro impacto menos tangible pero profundamente relevante de la auditoría informática es la generación de una cultura de seguridad organizacional. La literatura y los casos analizados muestran cómo el enfoque comunicativo y pedagógico de la auditoría incrementa la sensibilización del personal y promueve la adopción de buenas prácticas colectivas en materia de prevención, resiliencia y ética digital (5), (7), (13).

En empresas auditadas, Lizárraga Caipo destacan la realización frecuente de campañas de concienciación, simulacros de incidentes y formación permanente en ciberseguridad, lo cual disminuye tanto la frecuencia como la severidad de incidentes causados por errores humanos o desconocimiento (20). Además, la auditoría fomenta dinámicas de reporte voluntario de incidentes, lo que refuerza el aprendizaje organizacional y permite actuar con mayor celeridad ante eventos novedosos o amenazas emergentes.

Dentro de este proceso, la gestión del cambio adquiere un sentido positivo: la auditoría es vista como oportunidad de mejora y de adaptación frente a normativas, tecnologías y contextos cambiantes. Esto facilita la transición hacia modelos de madurez organizacional más robustos y una superior capacidad para enfrentar los retos del entorno digital en evolución (8).

Beneficios cuantificables y mejoras a largo plazo

Si bien muchos de los resultados obtenidos tienen un componente cualitativo, la literatura científica y los informes sectoriales consultados permiten contrastar mejoras y beneficios cuantificables derivados de la auditoría informática como se observan en la Tabla 1. En organizaciones con auditoría regular, la reducción de incidentes críticos puede ubicarse entre el 30% y el 45% según Arcentales y Jimbo-Santana (1), (2); el ahorro en gastos directos e indirectos relacionados a soporte tecnológico y respuesta a incidentes oscila entre el 10% y el 22% anual, y la percepción de satisfacción y confianza de usuarios internos mejora entre el 20% y el 30% en los ciclos posteriores a la auditoría sistemática (2), (5), (7), (10).

De igual modo, el tiempo de recuperación ante incidentes mayores (por ejemplo, caídas de sistemas core o secuestro de infraestructura tecnológica) se reduce hasta en un 50% luego de la implementación de controles automáticos y planes de contingencia derivados de auditorías [2]. La obtención de certificaciones internacionales pasa de menos del 40% en empresas no auditadas de modo sistemático, a superar el 90% en aquellas que incorporan la auditoría continua a su plan estratégico de seguridad (10).

Los sectores regulados, como banca, telecomunicaciones, salud y educación, reportan mayor estabilidad y menores sanciones regulatorias o pérdidas reputacionales tras adoptar auditorías recurrentes, según muestran tanto INTECO como organismos especializados en ciberseguridad (INCIBE, Red Clara, ISACA) (4), (10), (11), (12).

Desafíos en la implementación de la auditoría informática

A pesar de los beneficios comentados, la implantación de la auditoría informática sigue enfrentando retos y resistencias que pueden limitar su impacto si no se gestionan adecuadamente. Entre los obstáculos más relevantes identificados en la revisión, se encuentra la escasez de profesionales calificados, especialmente en regiones en desarrollo o en organizaciones pequeñas y medianas donde la formación especializada es un factor crítico (11), (12), (13). ISACA y Red Clara resaltan que la falta de expertos certificados en estándares internacionales es frecuente, lo que condiciona la calidad y profundidad de los ejercicios de auditoría interna y limita la autonomía tecnológica en países del sur global (11), (12).

La resistencia organizacional, a menudo asociada a la percepción de la auditoría como una instancia de control sancionador, puede derivar en ocultamiento de fallas, reportes incompletos o baja cooperación, afectando la validez y utilidad de los hallazgos (8), (11). Abordar este desafío requiere trabajar en la cultura organizacional, mejorar la comunicación interna e integrar a los equipos auditados en un proceso formativo y constructivo.

Las restricciones presupuestarias suponen otro desafío relevante: las auditorías requieren inversión en recursos humanos, tecnológicos y temporales. Organizaciones con presupuestos limitados tienden a relegar o simplificar las auditorías, lo cual incrementa el riesgo en contextos de alta exposición tecnológica y limita la capacidad de detección temprana de amenazas (2), (12).

Finalmente, la adaptación de marcos legales y normativos internacionales al contexto local y sectorial representa una barrera metodológica significativa. Estandarizar modelos como ISO/IEC, PCI DSS o GDPR, pensados para grandes organizaciones, implica procesos de contextualización y capacitación que exceden la mera traducción documental, exigiendo flexibilidad y formación continua tanto en el equipo auditor como en el auditado (6), (13).

La literatura revisada enfatiza la necesidad de estrategias sostenibles para la atracción y retención de talento auditor, la colaboración internacional y el desarrollo de guías y buenas prácticas a medida que apoyen la transferencia tecnológica y el aprendizaje mutuo.

Tendencias y mejores prácticas emergentes

De modo paralelo a los desafíos, la revisión documental identifica tendencias y mejores prácticas que están impulsando la evolución de la auditoría informática hacia formatos más eficientes, proactivos y adaptativos. Una de las tendencias destacadas es la automatización y digitalización progresiva del proceso auditor a través de la inteligencia artificial, machine learning, analítica avanzada y minería masiva de logs (13).

Empresas líderes han comenzado a implementar auditoría continua apoyada en aprendizaje automático, lo que permite detectar patrones de anomalías en tiempo real, correlacionar eventos y alertar sobre nuevas amenazas sin depender únicamente de revisiones periódicas manuales. Este enfoque incrementa la rapidez de reacción y la eficacia en la identificación de riesgos emergentes (13).

Otra línea de avance es la integración de estándares combinando requisitos de ISO/IEC 27001 con controles NIST y buenas prácticas de COBIT y la capacitación interdisciplinaria de auditores en ciberseguridad, análisis de datos y gestión del cambio, lo que favorece una visión holística del proceso auditor (7), (11), (13).

Es común el desarrollo de sistemas de gestión documental en la nube y la contratación regular de auditorías externas para asegurar independencia y benchmarking contra líderes del sector. Las mejores prácticas identificadas incluyen la formación anual obligatoria, el uso de incentivos

a la mejora continua y la colaboración con universidades, organismos reguladores y empresas del ámbito tecnológico (8).

En América Latina, iniciativas colaborativas entre universidades, organismos locales y expertos internacionales están acelerando la madurez de la auditoría informática, promoviendo el desarrollo de materiales didácticos, bancos de experiencias y la adaptación metodológica a realidades regionales (5), (12).

Casos de éxito internacionales y en Latinoamérica

La aplicación eficiente de la auditoría informática se refleja en casos documentados global y regionalmente. En la banca peruana, la instauración de una auditoría continua basada en ISO 27001 y COBIT derivó en una reducción del 40% en incidentes críticos, mejoras en satisfacción del cliente y un posicionamiento favorable ante reguladores (2), (5). En España, programas nacionales impulsados por INCIBE y la adopción extendida de auditorías en el sector salud han reducido sanciones regulatorias y fugas de datos en hospitales públicos y privados (4), (10).

En administración pública, experiencias en ciudades digitales en México y Chile evidencian mejoras en la digitalización segura de trámites, detección de anomalías y transparencia en la gestión de recursos públicos (12). Universidades latinoamericanas, en colaboración con europeos, han desarrollado equipos multidisciplinarios que transfieren conocimiento y diseño de guías propias, disminuyendo la dependencia de expertos externos y fortaleciendo la sostenibilidad del proceso auditor (5), (12).

DISCUSIÓN

La discusión de los resultados obtenidos permite establecer un análisis crítico de los beneficios y desafíos que supone la auditoría informática en las organizaciones modernas, así como reflexionar sobre el papel que desempeña como herramienta estratégica para la protección, buen gobierno y sostenibilidad de los procesos institucionales.

Los resultados confirman que la auditoría informática es un elemento sustancial para la mitigación de riesgos tecnológicos, como han destacado Jimbo-Santana et al. y Arcentales Fernández y Caycedo Casas (1), (2). El descenso sustantivo en incidentes críticos de seguridad registrado en instituciones auditadas bajo estándares reconocidos como ISO 27001 y COBIT 5 evidencia la eficacia de la auditoría sistemática, especialmente en sectores expuestos como el financiero, salud y administración pública. No obstante, estos hallazgos coinciden con investigaciones previas que enfatizan que el impacto real depende en gran medida de la adecuada aplicación de planes de mejora, la actualización constante de controles y la colaboración entre equipos técnicos y auditoría (7), (8). Esto resalta la importancia del liderazgo y la cultura institucional, tal como señalan Plastino et al. y el propio ISACA en estudios globales recientes [8,25]. Una auditoría enfocada solo en el cumplimiento formal, sin una apropiación real de las recomendaciones, corre el riesgo de convertirse en un trámite carente de efectos transformadores.

La mejora en eficiencia operativa y la optimización de procesos constituyen otro eje valioso, pero al mismo tiempo presentan retos de mayor alcance en organizaciones con estructuras rígidas o recursos limitados. Estudios como el de Morales (24) demuestran ahorros operativos considerables tras auditorías profundas, aunque alertan que parte de estos beneficios puede verse diluida si no se acompaña de políticas de actualización tecnológica y gestión documental permanente. Por tanto, el éxito de la auditoría informática no puede desligarse de la inversión sostenida en capacitación, actualización de infraestructura y mejora de procesos internos, así como de la alineación estratégica entre áreas de TI y dirección general.

En el ámbito del cumplimiento normativo, la auditoría informática se consolida como el principal mecanismo para la obtención y mantenimiento de certificaciones –destacando la robustez de este beneficio en contextos de fuerte regulación, como ilustran los informes de INTECO y la experiencia española y peruana (10), (5). La rápida evolución normativa internacional implica, sin embargo, nuevos desafíos: la necesidad de adaptar marcos extranjeros a realidades locales y gestionar la presión constante por mantener la conformidad frente a nuevos criterios de auditoría. En este sentido, la literatura revisada coincide en la urgencia de procesos de contextualización y flexibilidad metodológica, destacando el valor de los equipos interdisciplinarios y la cooperación con entidades externas para asegurar la aplicabilidad y pertinencia de los modelos de auditoría (6), (11), (13).

El apoyo de la auditoría informática en la toma de decisiones estratégicas sobresale como uno de los aportes mejor valorados por directivos y responsables de TI. Los informes y recomendaciones derivados del proceso auditor permiten argumentar inversiones, justificar presupuestos en ciberseguridad y establecer mejores prácticas adaptadas a riesgos emergentes. Coincidiendo con Plastino et al. (25) y la tendencia hacia la auditoría continua y el uso de analítica avanzada introduce nuevas oportunidades y desafíos: la automatización puede potenciar la prevención temprana y la transparencia, pero exige talento calificado para gestión y análisis de grandes volúmenes de datos.

Un elemento transversal observado es el impulso hacia la formación de una cultura de seguridad integral. Si bien la auditoría fomenta actitudes más proactivas y responsables en todos los niveles, existe evidencia de que la efectividad de este cambio cultural depende de la comunicación clara de los hallazgos y la integración de la auditoría como parte del aprendizaje y no como control externo punitivo (5), (7). Organizaciones que trasladan sus procesos de auditoría a iniciativas de capacitación, talleres y simulacros muestran mayores mejoras sostenidas y menor reincidencia de errores humanos.

Por otro lado, los resultados ponen de relieve los retos persistentes: la escasez de personal calificado en auditoría digital, la resistencia al cambio en sectores tradicionales y la dificultad de adaptar estándares tecnológicos universales a las singularidades organizacionales. Autores como ISACA y Red Clara señalan que la solución a estos puntos pasa por la colaboración internacional, la certificación continua de profesionales y el desarrollo de recursos didácticos y guías sectoriales adaptadas (16).

En síntesis, la auditoría informática aporta beneficios evidentes y cuantificables en seguridad, eficiencia, cumplimiento normativo y cultura organizacional, pero su sostenibilidad y valor estratégico solo se materializan plenamente cuando se integra como un proceso dinámico, contextualizado e inclusivo que involucra a toda la organización y se ajusta a la evolución constante del entorno digital.

CONCLUSIONES

Las evidencias analizadas en esta revisión confirman que la auditoría informática es actualmente un pilar esencial para la gestión eficaz de la seguridad, la eficiencia operativa y el cumplimiento normativo en organizaciones de todos los sectores. Su implementación periódica y estratégica genera una reducción sustancial de incidentes críticos y vulnerabilidades, permitiendo a las instituciones anticipar riesgos y fortalecer su resiliencia frente a amenazas digitales cada vez más complejas y dinámicas. Además, facilita la optimización de procesos, la transparencia documental y una mejora cuantificable en la satisfacción de usuarios internos y externos, aportando ventajas competitivas y sostenibilidad en contextos caracterizados por alta incertidumbre tecnológica.

Sin embargo, los beneficios de la auditoría informática alcanzan su máxima expresión sólo cuando se integran a una cultura organizacional enfocada en la mejora continua, la formación y la participación activa de todas las áreas. El éxito del proceso depende no solo de la rigurosidad técnica y el apego a estándares internacionales como ISO 27001 o COBIT, sino también de la capacidad para contextualizar recomendaciones, superar la resistencia al cambio y promover la colaboración interdisciplinaria. Las experiencias internacionales y latinoamericanas ilustran que la adaptación flexible y la inversión en talento humano son condiciones clave para consolidar la madurez y sostenibilidad de los mecanismos de control y gobierno digital.

Finalmente, la auditoría informática está en proceso de transformación gracias a tendencias emergentes como la automatización, la inteligencia artificial aplicada y la auditoría continua. Estas innovaciones tienen el potencial de agilizar la detección y gestión de riesgos, pero requieren igualmente un esfuerzo constante en capacitación, supervisión ética y contextualización normativa. Las organizaciones que asuman la auditoría informática no solo como función de control, sino como aliada estratégica, estarán mejor preparadas para afrontar los desafíos del entorno digital, garantizar su competitividad y responder de manera efectiva a la evolución de los marcos regulatorios y tecnológicos.

REFERENCIAS BIBLIOGRÁFICAS

1. Arcentales Fernández S, Caycedo Casas P. Auditoría informática: nuevas perspectivas y desafíos. Rev Científica Multidisciplinaria InvestiGo. 2017;13(2):125-139.
2. Avanzi R. Auditoría informática: bases teóricas y aplicación práctica. Madrid: Ediciones Académicas; 2020.

3. Calderón M, Silva J. Auditoría de Tecnologías de Información: prácticas y estándares internacionales. Gestión y Estrategia. 2018;34(1):77–89.
4. Cañete M, Salgado V. Evaluación del riesgo en auditoría informática: enfoque aplicado en pymes. Rev Virtual Universidad Católica del Norte. 2022;64:89-105.
5. CERT-IN. Guidelines for Information Security Audit. New Delhi: Indian Computer Emergency Response Team; 2021.
6. Díaz Martínez M, García Esteve C. Tendencias en auditoría digital: automatización e inteligencia artificial. Rev Española de Auditoría. 2023;59(3):84-97.
7. European Union Agency for Cybersecurity (ENISA). Good practices for Security of IoT. ENISA; 2019.
8. Florido Hernández M, Dueñas Rubira Á. Estado actual y tendencias en la auditoría de seguridad de la información. Revista de Tecnología e Innovación. 2022;7(2):36-50.
9. García M, Sáez J, Torres P. Implementación de marcos normativos en procesos de auditoría informática. Ciencia y Desarrollo. 2021;18(3):20-34.
10. Gómez O, Rodríguez J. Auditorías en la Administración Pública: lecciones aprendidas y nuevas perspectivas. Revista Española de Auditoría. 2020;58(4):12-34.
11. INTECO. Guía práctica de auditoría técnica de la seguridad. Madrid: INTECO; 2018.
12. INCIBE. Ciberseguridad en el sector sanitario: retos y buenas prácticas. INCIBE; 2020.
13. INCIBE. Guía de auditoría de la seguridad TIC. León: INCIBE; 2021.
14. International Organization for Standardization (ISO). ISO/IEC 27001:2022. Information Technology — Security Techniques — Information Security Management Systems — Requirements. Geneva: ISO; 2022.
15. ISACA. Control Objectives for Information and Related Technology (COBIT 5). Rolling Meadows: ISACA; 2019.
16. ISACA. Estado mundial del gobierno y la auditoría de TI. ISACA; 2023.
17. Jimbo-Santana LC, Gómez-Álvarez KD, Murillo-Quiroz AF. Auditoría informática y su impacto en la gestión de organizaciones financieras. Rev Ciencia Digital. 2023;7(2):24-36.
18. Kassem R, Higson A. The new audit regime in information systems: lessons from literature. Journal of Information Systems and Technology Management. 2019;16:e201916002.
19. Kemp F, Foster T. Cybersecurity Auditing: International Compliance and Future Challenges. International Journal of Information Security. 2021;20(2):105–26.
20. Lizárraga Caipo V, Medina Vásquez Y, Izquierdo Rivero I. Auditoría informática: impacto y beneficios en empresas peruanas. Idelca. 2022;23(7):1-17.
21. Lozano A, Díez M, García R. Revisión sistemática en administración y gestión: procedimientos y materiales. Rev Adm Iberolatinoam. 2020;48(6):70-81.
22. Ministerio de Administraciones Públicas de España. MAGERIT: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. 3ª ed. Madrid: MAP; 2020.
23. Moher D, Liberati A, Tetzlaff J, Altman DG, PRISMA Group. Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement. Ann Intern Med. 2009;151(4):264–9.
24. Morales Gortárez ME. Análisis de las tecnologías y normativas en auditoría informática. CIENCIAergosum. 2019;26(3):345-356.
25. Plastino A, Vázquez Sáez L, Navas Carrillo D. La auditoría informática: evolución, modelos y tendencias. Rev Científica UNED. 2021;35(5):123-145.

26. Red Clara. Madurez de la auditoría informática Latinoamérica: desafíos y avances. Red Clara; 2022.
27. SANS Institute. Introduction to IT Audit. Bethesda: SANS; 2021.
28. Silva P, Torres R. Big data, inteligencia artificial y el futuro de la auditoría de sistemas. Revista de Ingeniería Informática. 2022;14(1):52-68.
29. Universidad de las Américas. Auditoría informática en el sector salud. Quito: UDAL; 2021.
30. Universidad Europea. Auditoría informática: evolución, retos y competencias. Madrid: Universidad Europea; 2021.